Accellion Share Securely™

AN ACCELLION WHITE PAPER

5 Security Essentials for Collaboration in the Enterprise.

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com

Executive Summary

With the increasing use of collaboration tools in the enterprise, it is essential that organizations implement best practices and safeguards to ensure enterprise data security and compliance.

Managing the sharing of valuable information assets such as confidential intellectual property, sensitive customer data, financial information, product designs, and personal health information continues to be a top priority for all enterprises. Balancing enterprise data security and compliance requirements with user needs for easy, anytime, anywhere information access is a challenge that many organizations face.

This whitepaper explores the security hazards of unsecure and unmanaged collaboration, and provides an overview of the top 5 security essentials for any enterprise collaboration solution.

.

Introduction

Collaboration is not a new concept in the enterprise —it's been around as long as people have been working together. But now, in the age of cloud computing, mobile devices, and easy access to Software as a Service (SaaS), enterprise employees are collaborating differently. Employees with access to the Internet, a web browser, and the files on their desktop, are eagerly trying and using free or inexpensive collaboration tools for business use–without IT oversight or control. Dropbox-type solutions for syncing files between devices, wikis, and free file-sharing services are just some of the unsanctioned collaboration tools that are infiltrating the enterprise, putting the organization at risk for a data breach.

Unauthorized use of collaboration solutions poses enormous risks to enterprise data security and regulatory compliance.

Unauthorized use of collaboration solutions poses enormous risks to organizations in the area of enterprise data security and regulatory compliance. Many, if not most, of the files being shared on collaboration platforms contain confidential information, including business plans, customer records, financial reports, technology plans, partner agreements, and HR records. Files such as these present a data breach risk if they are exposed. If a data breach does occur, the consequences for the enterprise can be dire: regulatory penalties, public censure, customer defections, lost business, and loss of competitive advantage.

Balancing enterprise data security and compliance requirements with user needs for easy, anytime, anywhere information access—even from mobile devices—is a challenge for most organizations. So how can enterprises realize the many benefits of collaboration while mitigating data security and compliance risks?

The Benefits of Collaboration

Online communication and collaboration have evolved rapidly from their beginnings with email. Email created a revolution in how people communicate and set high expectations for speed and ease of use. Now content management systems, wikis, online chat, and internal blogging platforms have made it easier than ever for employees to share information, organize it, and converse online. This revolution in communication adds context that's missing from individual email messages, makes it easier to review a discussion in its entirety, and to discover how and why decisions have been made.

Today's collaboration tools cover a wide array of capabilities; however inherent in most is the ability to share files. The real value of collaboration almost always involves file sharing, since this is where the most valuable information resides.

Collaboration solutions offer several advantages over file sharing via the email paperclip, not least being that files are easier to find. A user doesn't have to dig through a thread of email messages in search of the latest working draft. The latest working draft is posted and clearly presented on a project page. Since knowledge workers spend 15-30% of their time just looking for information (IDC), making files easier to find can be a big productivity boost for any enterprise.[1]

The real value of collaboration almost always involves file sharing, since this is where the most valuable information resides.

Collaboration solutions offer other advantages, as well. Team members can post comments about files and tag them to make them more searchable. Instead of discussions being buried in email, they're centrally stored and posted for all authorized users to read.

File versioning, another common collaboration solution feature, allows team members to compare different versions of files and to make sure comments and discussions are referring to the same version.

A collaborative workspace can be configured to notify users of new files or comments, following a "push" communication model like email. At the same time, users can choose to visit the collaborative workspace whenever they like—and from wherever they like, if the solution supports mobile access—following a more accommodating "pull" model of communication.

However, while file sharing enriches collaboration, it also creates risk for the enterprise, since the loss of confidential data through collaborative file sharing can impose significant financial costs.

The Challenge of Enterprise Collaboration

Cross-boundary Collaboration

Collaboration—people working together—is a fluid activity, involving ever-changing groups of people of diverse backgrounds and skills. A collaborative team might be geographically distributed. It might also include employees from

[1] Spinuzzi, Hart-Davidson, and Zachry, "Modeling Knowledge Work," http://www.drc.utexas.edu/main/sites/default/files/040505-1.pdf

several different organizations that vary in size and in IT capabilities. The fluidity and diversity of collaboration creates challenges, because the ever-shifting boundaries of collaborative groups don't necessarily align with the boundaries of a single enterprise's IT infrastructure.

In business today, cross-boundary collaboration—that is, collaboration between internal users and external users—is increasingly the norm. Internal users need to work closely with external users such as remote call centers, outsourced manufacturers, distributors, resellers, logistics companies, ad agencies, and legal counsel. Sharing files with these diverse communities is essential for enterprise collaboration, yet difficult and expensive to accomplish with solutions such as SharePoint. Typically, SharePoint is configured only for internal collaboration. File access is limited to authorized users with internal email addresses. In addition, the application is typically licensed based on the number of seats or user accounts, and most enterprises are reluctant to purchase additional licenses for external users who may occasionally need to share files.

By failing to provision employees with secure file sharing, an enterprise increases the likelihood that data security will be breached by an unsecure file-sharing tool selected by employees.

Without SharePoint logins, trusted business partners—and even employees in other departments—can be shut-out from business-critical data they need to do their jobs. To make SharePoint content available to external users and users in other departments, an IT department can set-up external server farms storing copies of SharePoint data, but this duplication, which requires ongoing synchronization and maintenance, is time-consuming and expensive. In addition, these server farms are typically limited in functionality; for example, they typically don't support mobile access.

In the world of mobile, fluid, cross-boundary collaboration, the restrictions imposed by secure collaboration platforms can be counterproductive. Team members want to be productive, and file sharing is a necessity. When confronted with these account-based security limitations, many users seek work-arounds. The typical end-run: an authorized user downloads a file from the collaboration platform, and then blasts the file out to other team members over unsecured, unmonitored channels such as email, FTP, or the latest Web 2.0 startup specializing in file-sharing.

Security Risks of Collaboration

In this era of cloud computing and free or low-cost SaaS applications, it has never been easier for employees to gain access to tools for improving personal productivity. Under the category of collaboration tools, there is no shortage of free file-sharing services, including dropbox-type solutions that provide remote file syncing, free file-transfer and file sharing accounts that provide less restrictive file attachment limits than business email accounts, and even social networking sites like Facebook. Not to mention the fallback of sharing files via USB devices or CDs.

The problem with these file-sharing methods is that they are not secure. They lack controls for limiting data access; they usually forego encryption in transit, if not also encryption in storage; and they cannot be monitored and audited by IT and security departments. By failing to provision employees with secure file, an enterprise increases the likelihood that its data security will be breached, by an unsecure file-sharing tool selected by employees.

The data breaches associated with these unsecure file-sharing methods continually make headline news:

- USB sticks and CD ROMs are lost or stolen. (Example: Private First Class Manning stealing diplomatic cables for WikiLeaks.)
- FTP servers leave confidential files accessible indefinitely. (Example: A sheriff's department posting a list of informants on a public server.[2])
- Free consumer services for webmail and file-transfers are used to share confidential data; triggering regulatory violations by putting confidential data outside the control of the enterprise IT department.

Unsecure file-sharing routinely leads to data breaches, compliance violations, tarnished brands, identify theft, and fraud. Free and easy file sharing for employees becomes costly and difficult for the organization. Enterprises need a better solution.

Requirements for Secure Collaboration

Enterprises need a solution for secure information sharing that combines the ease of use and simplicity of email, with the rich features of contemporary collaboration solutions.

Enterprises need a solution for secure information sharing that combines the ease of use and simplicity of email, with the rich features of contemporary collaboration solutions. They need a solution that builds on their investment in internal collaboration platforms like SharePoint and Autonomy, while ensuring that employees can also collaborate with external users.

Secure collaboration needs to combine the flexibility and ease-of-use of today's consumer tools with the security and compliance associated with controlled and managed IT systems. The goal is to provide secure file sharing without sacrificing ease-of-use.

5 Security Essentials for Collaboration in the Enterprise

1. Encrypted file transfer and file storage
   Encryption is an essential best practice for data security. Files should be protected wherever they are—in transit or stored on a server. Collaboration solutions should apply encryption that's rigorous enough to survive brute force attacks and other attacks commonly used by hackers.
2. Authenticated access to files
   Authentication—verifying the identity of users before granting them access to content—is another best practice for security. To enforce authentication consistently, the collaboration solution should integrate with existing enterprise authentication systems, such LDAP.

[2] "New policy to prevent data breach," *The Daily Sentinel*, http://www.gjsentinel.com/news/articles/new_policy_to_prevent_data_bre

3. Comprehensive file tracking and reporting features for regulatory compliance with HIPAA, GLBA, SOX, FDA
   File tracking and reporting features enable IT and security teams to demonstrate compliance with industry regulations, to monitor user behavior, and to quickly spot anomalies that could signify a potential breach.

4. Cross-boundary communication with all authorized users, including internal and external users
   Data security should follow the natural flow of collaborative conversations that typically span internal and external communication.

5. Support for all file sizes and formats beyond traditional limits of email, 100 GB or more
   File sizes are growing dramatically thanks to the growing popularity of high-resolution graphics, video content, and other specialized content. In certain industries such as healthcare, where the practice of transmitting large files with medical images is becoming increasingly common, and advertising, where ad teams exchange large graphics files with clients and with production departments, the ability to share large files securely is a business necessity. By accommodating files of all sizes, a collaboration solution removes the temptation for users to seek an unsecure alternative for sharing very large files.

Simply put, an enterprise collaboration solution should enable users to share files of any size securely with the people they’re collaborating with, regardless of whether those people are local or remote, and all file-sharing activity should be able to be monitored and controlled for compliance with company policies and industry regulations. These capabilities are the security essentials for collaboration today.

Accellion Secure Collaboration

Accellion provides enterprise-class secure collaboration and managed file transfer solutions that provide the security essentials for enterprise collaboration.

Accellion Secure Collaboration™ makes it easy for enterprise users to share confidential information with their colleagues, clients, and partners while supporting enterprise security, compliance, and improved business productivity. Accellion enables collaborators to quickly, easily, and securely share files from anywhere, at any time on virtually any device by providing access to secure workspaces to share and comment on files and track file versions. The employee who creates a workspace becomes its manager and assigns access privileges to other users, including external users in other domains. These fine-grained access controls include determining who can share files, who can comment on files, and who can download files.

The encryption, authentication, and audit trail features provided by Accellion Secure Collaboration enable enterprises to demonstrate compliance with government and industry regulations including GLBA, HIPAA, SOX, and FDA. For more information and additional resources on Accellion Secure Collaboration, please visit: http://www.accellion.com/products-services/secure-collaboration

Accellion Secure Collaboration and Managed File Transfer solutions also support integration with existing enterprise systems including Microsoft SharePoint, Outlook, OCS, Autonomy iManage, and Lotus Notes. In addition, Accellion solutions can be easily integrated with enterprise DLP systems from Symantec, RCA, Fidelis, Code Green Networks and Palisades. The Accellion solution achieves effective security and compliance by augmenting those enterprise applications with enhanced security features that are convenient and easy-to-use for the business user.

Key Benefits of the Accellion Solution:

- Easy-to-Use: enterprise users can share project files, images, presentations, spreadsheets, financial documents, product specifications, and any file or folder up to 100 GB in size, quickly, easily and securely with both internal and external stakeholders.
- Flexible, Scalable Deployment: Accellion offers the widest breadth of deployment options enabling enterprises to balance cost, security, and speed of deployment for a single office or multiple distributed offices around the globe. Accellion supports deployment in VMware, Citrix XenServer, and Microsoft HyperV virtual environments, choice of public, private, or hybrid cloud deployments and FIPS 140-2 certified deployments.
- Mobile Access: users can view, comment on and share files via a laptop, smartphone or Web-enabled device, from native mobile applications for the iPhone, iPad, Android and BlackBerry.
- Enhances Current IT Investments: integration with Microsoft SharePoint, OCS and other business applications means getting the most out of technology investments.
- Compliance: ensures compliance with industry and government regulations including SOX, GLBA, HIPAA, and FDA.

Accellion Secure Collaboration and File Transfer solutions are used by leading enterprise organizations including Procter & Gamble; Activision; Clarian Health Partners; Kaiser Permanente; Foley & Mansfield; Lovells; Bridgestone; Ogilvy & Mather; Harvard University; Guinness World Records; US Securities and Exchange Commission; and NASA.

For more information, please visit www.accellion.com or call +1 650-485-4300.